ANSWERING BRIEF TO DEFENDANT'S MOTION FOR PARTIAL SUMMARY JUDGMENT EXHIBIT 10

Marketing Services

Fraud and Identity Management

Risk Management

Collections Management

Credit Reporting

Data Compromise Assistance

Online Applications

Data Compromise Assistance

You know how important it is to protect your customers' personal information. A crucial part of safeguarding information is being prepared to react quickly and e in the event of a data breach, security compromise or the identity theft of your c Doing so helps protect and retain customers and increases consumer confiden brand.

React faster with a customized solution

Our Data Compromise Assistance provides you with the strategy necessary to react quickly to these situations. We work with you to design a proactive solution that helps you react faster to fraud and reduce risks to your organization and your affected customers.

Be prepared to ac quickly if your customer's sensit personal informat compromised thro theft or inadverte of data records.

Fine-tune your response

With a more comprehensive suite of capabilities, you can reduce risks and take additional action to improve your customers' confidence. Our services can help you determine more effective strategies:

Credit Monitoring—Provide your customers with a credit report and notificati them identify any changes in their credit history and uncover suspicious activi be indicative of identity theft. Monitoring services can also help them regularly their status, while trained specialists are available in case of identity theft.

Compromise Warning Flag—Quickly identify if a consumer has been victimi identity theft to counter unauthorized use of an individual's sensitive personal information. A warning flag is placed on a consumer's credit report to help you organization and the consumer reduce additional risks, while minimizing your inconvenience.

NEXT STEPS:

Request more information on Data Compromise Assistance

Marketing Services

Fraud and Identity Management

- Identity Verification
- Authentication
- Compliance
- Fraud Response Services

Risk Management

Collections Management

Credit Reporting

Online Applications

Identity Verification

Confirm who is on the other side of your transaction by using an automated env to access multiple data sources and verify current customer identities. Predict th likelihood of fraud with advanced models and tools that flag high-risk informatio addresses, phone numbers and Social Security numbers.

Reduce the rate of false positives and manual error, thus improving return on investment and increasing customer satisfaction.

Determine the val information throughout your customer lifecycle

Take full advantage of fraud and identity management tools

Using powerful fraud models and advanced technologies, information is verified against vast databases, including one of the industry's most complete national files of p fraudulent information. These tools are available as stand-alone solutions or as report add-ons, providing you with an effective, convenient way to reduce the ri fraud.

NEXT STEPS:

Request more information on Identity Verification

PC Containing Consumer Credit Data Stolen

TransUnion will review its data handling processes after loss of desktop system with information on more than 3,600 consumers

By Tony Kontzer
InformationWeek
November 9, 2005 05:00 PM

With federal legislators mulling over options for fighting identify theft and fraud, TransUnion LLC, one of three companies that maintain consumer credit histories, provided the latest scare Wednesday, revealing that a password-protected PC containing personal credit information on more than 3,600 consumers was stolen from a regional sales office in California last month.

TransUnion's disclosure follows a string of compromised **data** incidents that have hit companies such as Bank of America, CardSystems Solutions Inc., ChoicePoint Inc., Citigroup, and HSBC North America, as well as numerous universities.

Upon learning of the theft, TransUnion promptly sent notices to 3,623 consumers last month alerting them to the breach and offering complimentary monitoring of credit reports for a year. The Chicago-based company also notified local law enforcement, and launched an internal investigation into the incident. The focus of that internal investigation is to find out why the information was stored on a far-flung PC rather than on TransUnion's **secure network**, says a company spokesman.

The spokesman says TransUnion also will take a close look at its internal security and data-handling processes. Initial indications are that the burglary was centered on the computer itself, not the data within it. While a portion of the information was encrypted, "some data may have been stored in a back-up file on an unencrypted portion of the computer's hard drive," the spokesman said in an E-mail.

The TransUnion breach comes less than a week after Microsoft (NSDQ: MSFT) chief counsel Brad Smith told the Congressional Internet Caucus that the software giant supports comprehensive legislation to tackle data privacy issues at the federal level. Smith suggested a four-part piece of legislation that would mandate baseline standards, more transparent data collection practices, individual control over use and disclosure of personal information, and minimal security requirements around storage of sensitive consumer data.

TransUnion and its two rivals in the consumer credit-history market, Equifax and Experian, said in September that they would work together on development of an encryption standard they would all use to protect consumer data as it's moved between information providers and within the companies themselves. Last month, TransUnion made its fraud and identity management products available for mortgage lenders to integrate into their loan origination and underwriting systems.

Be afraid of the catastrophic data breach

By Ed Parry, Contributor
01 Dec 2005 | SearchSecurity.com

RSS FEEDS: Security Wire Daily News

Data breaches seem to be getting more common, and soon they could get more costly. At least one security analyst predicts that a breach will bankrupt a high-profile company.

Bank of America Corp., CardSystems Inc., ChoicePoint Inc., LexisNexis Group and TransUnion LLC represent just a handful of the most recent victims bitten by the breach bug. But the lessons these high-profile companies are learning about customer data security may not be motivating other firms to secure their systems.

Many companies have not spent enough money on protection, according to Jon Oltsik, senior analyst with Enterprise Strategy Group in Milford, Mass. "They're playing catch-up now, but some say they will just live with the risk," he said. "Some old-school types can't justify the return on their investment."

Oltsik believes this ROI-based resistance will mean a new chapter in data security -- Chapter 11. He believes that a data breach will drive a large public company into bankruptcy within the next couple of years. "It's only going to get worse," he warned.

As further proof, a recent Ponemon Institute survey of 9,000 people found that 12% of respondents had been notified of a data breach or loss by a company with which they did business. Of those affected, 20% said they immediately stopped doing business with the companies that couldn't keep their data secure.

Costly consequences
CardSystems and ChoicePoint already have paid heavy prices for their breaches. Visa and American Express both dropped CardSystems after the Atlanta-based payment processor was hacked last summer, exposing more than 40 million credit card numbers.

"CardSystems' entire business viability is threatened," said Jonathan Penn, an analyst with Cambridge, Mass.-based Forrester Research Inc.

ChoicePoint took a $6 million charge in June after ID thieves duped the company into releasing personal data, exposing the information of as many as 162,000 Americans. The Alpharetta, Ga.-based data firm spent nearly $2 million contacting affected customers and offering them credit reports and monitoring services. ChoicePoint also saw its stock price fall after the breach and now faces a possible class action lawsuit.

The cost of disclosure, notification and the offer of credit monitoring services to affected users or customers after a breach can really add up. Penn said that the general rule is $15 per customer. "If it's a financial firm and credit cards are involved, that's an additional $35 for credit card replacement."

Chicago-based TransUnion suffered a breach in October when someone broke into a California sales office and stole a computer that might have contained credit information on approximately 3,600 customers. According to a statement, the company set up a toll-free hotline for affected consumers, let them request a free copy of their credit report from all three nationwide credit bureaus and gave them a free year of credit monitoring on all three credit reporting files. The company did not put a price tag on the damage control.

Millions affected

Data breaches in 2005 and people estimated to be affected.

< TR>

Companies	People affected
CardSystems	40 million
CitiFinancial	3.9 million
DSW/Retail Ventures	1.3 million
BofA	1.2 million
BofA, Wachovia, PNC Financial and Commerce Bancorp	676,000
Time Warner	600,000
Georgia DMV	465,000
Ameritrade	200,000
ChoicePoint	162,000
Boeing	161,000

Source: Privacy Rights Clearinghouse

TransUnion claimed that there was no indication of any fraudulent activity as a result of the burglary. According to company officials, identity theft is not a given after a breach.

"There is often a misconception that a compromise means identity theft is right around the corner," said Tim Keller, TransUnion's director of fraud and identity management solutions. "Many times, there's no evidence that information has fallen into the wrong hands – the key is to communicate with customers and address their concerns."

Lessons learned

Some 300,000 compromised passwords at LexisNexis were costly, but in the end might actually benefit the company.

While the Dayton, Ohio-based information company paid for a notification program and credit management consumer services, company officials did learn a valuable lesson.

"It brought home to us that customers needed to be more vigilant about their password protections," said Judi Schultz, the company's senior PR manager. The company now requires customers to change their passwords every 90 days.

Similarly, Bank of America, which lost backup tapes containing data on 1.2 million federal employees earlier this year and fell victim (along with several other banks) to dishonest insiders, has implemented a security program called SiteKey on its Web site. Intended to provide an additional authentication layer, customers are told not to enter their password unless they either see a specific image and message, or answer a series of confirmation questions.

Beyond financial and reputational consequences, data breaches undermine the public's confidence in online shopping and banking. Oltsik said even if a person's identity isn't stolen, he still pays in terms of privacy regulation, lost time, lost confidence and increased feelings of insecurity, all of which are proxies for money,. But he does believe that by and large, security in the digital age is coming around.

"We were so gaga over Internet connectivity over the years that we forgot we were making it easier to steal information," he said. "Now we're catching up."

http://www.pfizer.com/contact/pfizer_data_breach_faqs.jsp#Q10-2

True link from September 6th

FAQs Related to Pfizer Data Breach: FAQs

Questions

Answers

How was my information lost?

It appears the breach developed when a Pfizer employee wrongfully removed copies of confidential information from a Pfizer computer system late last year. This was done without Pfizer's knowledge or consent and in violation of Pfizer policy. Authorities are continuing to investigate the incident and Pfizer is taking steps to protect your security and privacy.

What information was lost?

The review is not complete, but Pfizer believes that in addition to your name and Social Security Number and/or Taxpayer Identification Number, some of the following information also may have been exposed: home address; home and/or cellular phone number(s); fax number; e-mail address, credit card number; bank account number; passport number; driver's license number; military identification number; birth date; signature; and reason for termination of Pfizer employment (if applicable).

Has the information been misused?

So far, there is no indication that any unauthorized person has misused or is misusing any of this information.

What are you doing to make sure this doesn't happen again?

Pfizer is doing an extensive review of its privacy and data security program and making changes that will further enhance its protection of privacy and its handling of sensitive information.

Additionally, Pfizer has engaged the services of Identity Safeguards, a firm that specializes in identity protection services. These services include 24 months of credit monitoring, reimbursement for lost income and expenses due to an identity theft incident, and complete restoration if you experience identity theft. Pfizer is paying for these services on your behalf.

Who should I contact if I have questions?

You should contact Identity Safeguards at 800-981-7578 for more information about the protection services that the company offers.

What steps can I take to reduce the chance that my information will be misused?

Consider signing up for Identity Safeguards Protection Program. Services include 24 months of credit monitoring, reimbursement for lost income and expenses due to an identity theft incident, and complete restoration if you experience identity theft. To register for these services, you will need the PIN printed in the notification letter. This will make it possible for you to complete the validation process and receive the protection package.

Activate your credit monitoring. This is part of the service you receive after enrolling with Identity Safeguards. However, you need to activate it personally for it to be effective. Specific instructions for activating your credit monitoring will be provided once you enroll with Identity Safeguards. Activating your credit monitoring will also allow you immediate access to your credit report online.

Consider placing a "fraud alert" on your credit file. On request, any of the three nationwide consumer credit reporting companies can place a fraud alert in your file to alert potential creditors that you may be a victim of identity theft; a fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to

protect you – however, it may also delay your ability to obtain credit if you are applying for a credit card or other form of credit.

What is Identity Theft?

According to the United States Department of Justice, the terms *identity theft* and *identity fraud* "refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."

It is important to remember that a breach of your personal information does not mean you will experience identity theft.

What is credit monitoring?

Monitoring your credit reports regularly is your first line of defense. Credit monitoring is a very effective tool for becoming aware of fraudulent activity immediately. Every week, you'll be informed of changes to your credit report, alerting you to activities such as:

- New inquiries
- New accounts opened in your name
- Late payments
- Improvements in your report
- Bankruptcies and other public records
- New addresses
- New employers

How can I activate the credit monitoring and receive a credit report?

Explicit instructions are provided in your notification letter. If you need assistance, please contact Identity Safeguards at 800-981-7534.

What does the credit monitoring activation process involve?

You will be ordering a copy of your credit report and enrolling for a weekly credit monitoring service online. Part of this process requires True Credit to verify your identity. They will ask for personal protection information such as social security numbers, previous address, etc. Do not be concerned about entering this information into the True Credit website. They already have it and are just using it to verify your identity.

You will receive the True Credit certificate code to register for this service, which you received in your Identity Safeguards enrollment package. You will not be required to pay for anything. This process will take approximately 15 to 30 minutes to complete, and afterward you will have unlimited access to your credit report. Credit monitoring will then begin.

The service offering from Pfizer includes 2 years of credit monitoring, but the language on the True Credit website seems to suggest that I will be getting credit monitoring for one year only. What is the explanation?

Your Identity Safeguards membership, provided by Pfizer, is valid for 2 years. As a part of your membership, you will receive two certificate codes for credit monitoring services through TrueCredit. Each certificate code is good for one year. When you register for the first time with Identity Safeguards, you receive your first certificate code. When the time comes to register for another year of credit monitoring services with True Credit, IDS will provide you with a new code for easy reactivation.

How do I set a fraud alert?

The easiest way to contact one of the credit bureaus via the web is to visit http://www.experian.com/

Click on "Steps to take if you are a victim of fraud or identity theft" on the bottom of the page under the heading "Preventing Fraud."

You will answer some questions to confirm your identity, and then a 90-day security alert will be added to your credit file. Experian will give you access to view your report online. You should examine it carefully for accuracy. Experian will also share this information with Equifax and TransUnion who will both mail you confirmation letters containing a number to call to order complimentary copies of your credit reports for review.

To contact one of the credit bureaus by phone, see the numbers below:

Equifax: (800) 525-6285
Experian: (888) 397-3742
TransUnion: (800) 680-7289

It is only necessary to contact one of these bureaus and use one of these methods.

You will not be charged for this service. Please note placing a fraud alert may delay your ability to open new lines of credit quickly. Please activate the credit monitoring service before setting fraud alerts. This makes the process faster and easier.

Why should I set a fraud alert with the Credit Bureaus?

This will help prevent someone from opening new accounts in your name. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts as well. All three bureaus will mail you a confirmation letter and you will be able to order complimentary credit reports for your review.

You will not be charged for this service. Please note that placing a fraud alert may delay your ability to open new lines of credit quickly. You should activate credit monitoring before setting fraud alerts to ensure faster and easier processing.

What expense does Identity Safeguards Protection Program cover?

Those enrolled will receive Identity Safeguards credit monitoring for 2 years. If you experience a fraud or identity theft, you will receive help from an Identity Safeguards Recovery Advocate to restore your identity to a pre-event status. You are also eligible for lost income and expense reimbursement, with no deductible. Identity Safeguards provides coverage for lost income (time off work) and expenses (e.g., credit reports, legal fees for some civil suits, fees for refilling loan applications) related to the recovery process. There are no additional charges for this service.

What does the Recovery Advocate do?

If a participant becomes a victim of identity theft, Identity Safeguards assigns a Recovery Advocate to manage the case from beginning to end. Your Recovery Advocate does a great deal of work so you can remain productive at work and at home. Identity Safeguards disputes all fraudulent charges, contacts affected merchants, deals with collection agencies and works on your behalf to correct the problem. This service continues until your pre-event credit status is re-established. Your Recovery Advocate will be your main contact and source of information during this time.

What can I expect when recovery is done?

Once your case is closed, it will stay in Identity Safeguards' system for 36 months. If any other events stem from your unique identity theft case, they will re-open and take care of it. You will have access to Recovery Advocates if you ever have a question or concern.

Top

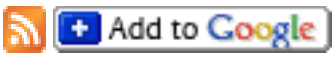
Updated September 6, 2007

From: Tech Gal [techgal69@sbcglobal.net]
Sent: Thursday, October 25, 2007 6:18 PM
To: Joyce@joyceyeagerlaw.com
Subject: TU Data Breech Aritcle

Be afraid of the catastrophic data breach

By Ed Parry, Contributor
01 Dec 2005 | SearchSecurity.com

RSS FEEDS: Security Wire Daily News



Data breaches seem to be getting more common, and soon they could get more costly. At least one security analyst predicts that a breach will bankrupt a high-profile company.

Bank of America Corp., CardSystems Inc., ChoicePoint Inc., LexisNexis Group and TransUnion LLC represent just a handful of the most recent victims bitten by the breach bug. But the lessons these high-profile companies are learning about customer data security may not be motivating other firms to secure their systems.

Many companies have not spent enough money on protection, according to Jon Oltsik, senior analyst with Enterprise Strategy Group in Milford, Mass. "They're playing catch-up now, but some say they will just live with the risk," he said. "Some old-school types can't justify the return on their investment."

Oltsik believes this ROI-based resistance will mean a new chapter in data security -- Chapter 11. He believes that a data breach will drive a large public company into bankruptcy within the next couple of years. "It's only going to get worse," he warned.

As further proof, a recent Ponemon Institute survey of 9,000 people found that 12% of respondents had been notified of a data breach or loss by a company with which they did business. Of those affected, 20% said they immediately stopped doing business with the companies that couldn't keep their data secure.

Costly consequences

CardSystems and ChoicePoint already have paid heavy prices for their breaches. Visa and American Express both dropped CardSystems after the Atlanta-based payment processor was hacked last summer, exposing more than 40 million credit card numbers.

"CardSystems' entire business viability is threatened," said Jonathan Penn, an analyst with Cambridge, Mass.-based Forrester Research Inc.

ChoicePoint took a $6 million charge in June after ID thieves duped the company into releasing personal data, exposing the information of as many as 162,000 Americans. The Alpharetta, Ga.-based data firm spent nearly $2 million contacting affected customers and offering them credit reports and monitoring services. ChoicePoint also saw its stock price fall after the breach and now faces a possible class action lawsuit.

The cost of disclosure, notification and the offer of credit monitoring services to affected users or customers after a breach can really add up. Penn said that the general rule is $15 per customer. "If it's a financial firm and credit cards are involved, that's an additional $35 for credit card replacement."

Chicago-based TransUnion suffered a breach in October when someone broke into a California sales office and stole a computer that might have contained credit information on approximately 3,600 customers. According to a statement, the company set up a toll-free hotline for affected consumers, let them request a free copy of their credit report from all three nationwide credit bureaus and gave them a free year of credit monitoring on all three credit reporting files. The company did not put a price tag on the damage control.

Millions affected

Data breaches in 2005 and people estimated to be affected.

< TR>

Companies	People affected
CardSystems	40 million
CitiFinancial	3.9 million
DSW/Retail Ventures	1.3 million

TransUnion claimed that there was no indication of any fraudulent activity as a result of the burglary. According to company officials, identity theft is not a given after a breach.

"There is often a misconception that a compromise means identity theft is right around the corner," said Tim Keller, TransUnion's director of fraud and identity management solutions. "Many times, there's no evidence that information has fallen into the wrong hands – the key is to communicate with customers and address their concerns."

BofA	1.2 million
BofA, Wachovia, PNC Financial and Commerce Bancorp	676,000
Time Warner	600,000
Georgia DMV	465,000
Ameritrade	200,000
ChoicePoint	162,000
Boeing	161,000

Source: Privacy Rights Clearinghouse

Lessons learned

Some 300,000 compromised passwords at LexisNexis were costly, but in the end might actually benefit the company.

While the Dayton, Ohio-based information company paid for a notification program and credit management consumer services, company officials did learn a valuable lesson.

"It brought home to us that customers needed to be more vigilant about their password protections," said Judi Schultz, the company's senior PR manager. The company now requires customers to change their passwords every 90 days.

Similarly, Bank of America, which lost backup tapes containing data on 1.2 million federal employees earlier this year and fell victim (along with several other banks) to dishonest insiders, has implemented a security program called SiteKey on its Web site. Intended to provide an additional authentication layer, customers are told not to enter their password unless they either see a specific image and message, or answer a series of confirmation questions.

Beyond financial and reputational consequences, data breaches undermine the public's confidence in online shopping and banking. Oltsik said even if a person's identity isn't stolen, he still pays in terms of privacy regulation, lost time, lost confidence and increased feelings of insecurity, all of which are proxies for money,. But he does believe that by and large, security in the digital age is coming around.

"We were so gaga over Internet connectivity over the years that we forgot we were making it easier to steal information," he said. "Now we're catching up."

Sound Off! - Be the first to post a message to Sound Off!

Share - Digg This! Bookmark with Del.icio.us